UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICHAEL BLAND, individually and on behalf of all others similarly situated, Plaintiff, v. UROLOGY OF GREATER ATLANTA, LLC a Georgia limited liability company Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff MICHAEL BLAND ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant UROLOGY OF GREATER ATLANTA ("UGA") based upon personal knowledge as to himself and his own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of his attorneys.

NATURE OF THE ACTION

1. From August 8 to August 29, 2021, Defendant UGA had their data servers breached by unauthorized third-party hackers, who stole the highly sensitive personal and medication information—including, *inter alia*, the full names,

addresses, dates of birth, age, dates of service, patient account numbers, diagnoses and treatment, and medical histories—of approximately 79,795 of its patients.[1]

2. UGA is a HIPAA healthcare provider that offers a wide variety of urological service to patients throughout the state of Georgia. As a requirement to procure its services, Defendant require that its patients provide them with their Personal Identifying Information ("PII") and Protected Health Information ("PHI"). As a result, Defendant collects and stores the PII and PHI of tens of thousands of individuals who have utilized its services.

3. Under statute and regulation, UGA had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect patient PII and PHI. UGA failed to do so. Notably, UGA explicitly promises in its public-facing Privacy Policy that "[w]e will obtain your express written authorization before using or disclosing your information for any other purpose not described in this notice."[2] Despite this, UGA did not obtain its patients' consent before allowing their information to be accessed and exfiltrated by unauthorized third-party hackers.

4. Plaintiff, individually and on behalf of those similarly situated persons (hereafter "Class Members"), brings this Class Action to secure redress against UGA for its reckless and negligent violation of their privacy rights. Plaintiff and Class Members are patients and former patients of UGA who had their PII and PHI collected, stored and ultimately breached by UGA.

5. Plaintiff and Class Members have suffered injuries and damages. As a result of UGA's wrongful actions and inactions, Plaintiff and Class Members' PII

[1] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed January 9, 2023).
[2] *Privacy Policy*, https://ugatl.com/privacy/ (last accessed January 9, 2023).

and PHI have all been compromised. Plaintiff and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes. Plaintiff and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiff and Class Members have also lost the value of their PII and PHI.

6. Further, Defendant unreasonably delayed in notifying Plaintiff and Class Members of the data breach until approximately November of 2022, despite having discovered the breach in August of 2021—over one year later.

7. As a result of UGA's wrongful actions and inactions, patient information was stolen. Plaintiff and Class Members who have had their PII compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Plaintiff and Class Members bring this action to secure redress against UGA.

THE PARTIES

8. Plaintiff Michael Bland is a Georgia citizen residing in McDonough, Georgia. Plaintiff is a former patient of UGA. On or around November 29, 2022, Plaintiff received a data breach notice from UGA informing him that his PII and PHI had been implicated in the data breach.

9. Urology of Greater Atlanta, LLC is a Georgia limited liability company company with its principal place of business at 290 Country Club Drive, Suite 10, Stockbridge, GA 30281. UGA's registered agent for service of process is located at that same address.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because upon the original filing of this complaint, members of the putative Plaintiff class reside in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds $5 million.

11. The Court also has personal jurisdiction over the Parties because Defendant routinely conducts business in the state of Georgia and has sufficient minimum contacts in Georgia to have intentionally availed themselves to this jurisdiction by operating and marketing its services in Georgia.

12. Venue is proper in this District because, among other things: (a) Plaintiff Bland is a resident of this District and a citizen of this state; (b) Defendant is a resident of this District and directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District for services provided in this district.

13. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Plaintiff resides in the Northern District, (b) Defendant conducts substantial business in the Northern District, (c) Defendant directed its services at residents in the Central District; and (d) many of the acts and omissions that give rise to this Action took place in the Northern District.

FACTUAL ALLEGATIONS

A. The Data Breach

14. Defendant UGA is a HIPAA healthcare provider that provides a variety of urological services to patients in the greater Atlanta area. As a requirement to procure its services, Defendant requires its patients to provide it with their sensitive

PII and PHI. As a result, Defendant's systems store the PII and PHI of tens and thousands of patients who have utilized its urological services.

15. From approximately August 8 to August 29, 2021, UGA's systems were accessed by unauthorized third-party hackers, who exfiltrated Plaintiff's and Class Members' sensitive PII and PHI—including, *inter alia*, their full names, addresses, dates of birth, age, dates of service, patient account numbers, diagnoses and treatment, an medical histories— from UGA's data servers. In its data breach notification filed the United States Secretary of Health and Human Services, UGA reported that the data breach had affected 79,795 individuals.[3]

B. Defendant's Unreasonably Delayed and Inadequate Notification

16. UGA owed Plaintiff and Class Members a duty under state and federal law to provide timely notification of the data breach. Under Georgia Code §10-1-912(a) *et seq.*, UGA was required to notify "any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person," and provide such notice "in the most expedient time possible and without unreasonable delay."

17. Likewise, UGA was also required under 45 CFR §164.404(b) to provide such notification "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."

18. In its Data Breach Notice sent to Plaintiff, UGA claims that it discovered the data breach on or around August 29, 2021. However, UGA did not begin notifying Plaintiff and Class Members until on or around November 28, 2022—over an entire year later.

[3] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited January 9, 2023).

C. UGA's Failure to Provide Reasonable, Adequate, and Compliant Data Security

19. UGA clearly recognized its duty to provide reasonable data security for Plaintiff's and Class Members' PII/PHI that it collects and stores as part of its business practices. UGA's privacy policy specifically promises that "[w]e will obtain your express written authorization before using or disclosing your information for any other purpose not described in this notice."."[4]

20. Despite this promise, UGA did not implement reasonable data security safeguards and protocols to protect Plaintiff's and Class Members' PII/PHI, and did not obtain Plaintiff's and Class Members' express authorization to disclose their PII and PHI, but ultimately did disclose that information to unauthorized third-party hackers.

D. UGA's Obligation to Protect Patient PII/PHI Under State and Federal Law

21. The duty of businesses such as UGA to protect the PII and PHI that its patients entrust to it is recognized under Georgia law, which states that the "[i]mplementation of technology security plans and security software as part of an information security policy" should be done to "provide protection to consumers and the general public from identity thieves." Georgia Code §10-1-910(4).

22. Further, as a HIPAA healthcare provider, UGA holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Member's PII/PHI.

23. Under the HIPAA Privacy Rule, UGA is required to:

a. Ensure the confidentiality, integrity, and availability of all

[4] *Privacy Policy*, https://ugatl.com/privacy/ (last accessed January 9, 2023).

electronic protected health information the covered entity or business associate creates, receives maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

45 CFR §164. 306(a)

24. The HIPAA Privacy Rule also requires UGA to "review and modify the security measures implemented…as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. §164.306(e) and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" under 45 C.F.R. §164.312(a)(1).

25. Further, the Federal Trade Commission Act, 45 U.S.C. §45 prohibits UGA from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

26. UGA failed to comply with each of these state and federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiff and Class Members' PII/PHI.

E. Applicable Standards of Care

27. In addition to their obligations under state and federal law, UGA owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. UGA owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII of Plaintiff and Class Members.

28. UGA owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

29. UGA owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed the PII in their possession, including adequately training their employees and others who accessed PII in their computer systems on how to adequately protect PII.

30. UGA owed a duty of care to Plaintiff and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

31. UGA owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

32. UGA owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard

individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII/PHI to UGA.

33. UGA owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

34. UGA owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. UGA received PII/PHI from Plaintiff and Class Members with the understanding that Plaintiff and Class Members expected their PHI/PII to be protected from disclosure. Defendants knew that a breach of its data systems would cause Plaintiff and Class Members to incur damages.

F. Stolen Information Is Valuable to Hackers and Thieves

35. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendant opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiffs and Class Members.

36. Plaintiffs and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

37. Legitimate organizations and criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

38. PII/PHI is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps."[5]

39. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

40. In addition to PII/PHI, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[6]

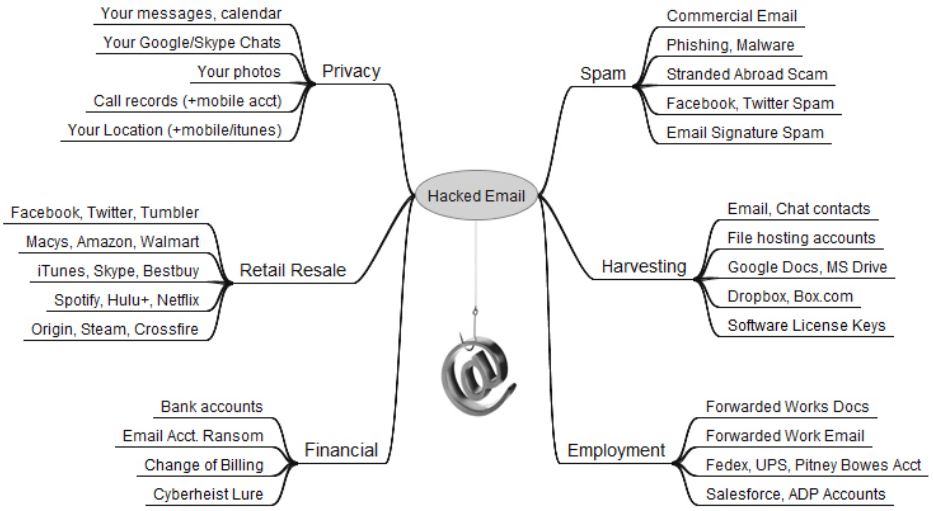
41. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[7]

---

[5] *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/ (last accessed January 10, 2023).

[6] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data. (last accessed January 10, 2023).

[7] Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/ (last accessed January 10, 2023).



42. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[8]

G. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

43. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and the Class

[8] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (last accessed January 10, 2023).

Members. The ramification of Defendant's failure to keep Plaintiffs and the Class Members' data secure is severe.

44. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[9] In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[10] The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the "worst ever year" for healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.[11]

45. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[12] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

---

[9] *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/. (last accessed January 10, 2023).

[10] *December 2019 Healthcare Data Breach*, HIPAA Journal (Jan 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed January 10, 2023).

[11] "Largest Healthcare Data Breaches of 2021," HIPPA Journal (Dec. 30, 2021), https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/ (last accessed January 10, 2023)

[12] *See Victims of Identity Theft*, U.S. Department of Justice (September 2015, revised November 13, 2017), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last accessed January 10, 2023).

H. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

46. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last accessed December 2, 2022.)

47. This is particularly the case with HIPAA data breaches such as Defendant's, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[13] Victims of medical identity theft "often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

[13] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/. (last accessed January 10, 2023).
[14] *Id.*

48. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[15] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[16]

49. Plaintiff and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

I. Plaintiffs and Class Members Suffered Damages

50. The exposure of Plaintiff and Class Members' PII/PHI to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. The data breach was also a result of Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and state and federal law.

---

[15] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/. (last accessed January 10, 2023).

[16] *Id.*

51. Plaintiff and Class Members' PII/PHI is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiffs and Class Members' consent to disclose their PHI/PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

52. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

53. Plaintiff has also lost the value of their PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

54. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo email accounts have been

listed for as little as $0.41, while banking logins are in the range of $500, and verified Paypal accounts with high balances are listed at as much as $2,000.

55. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70
Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

56. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and PHI, including information, such as a Social Security Numbers or diagnosis and medical treatment information, that is not easily, or outright cannot be changed in response to a data breach. As a result, a healthcare data record may be valued at up to **$250 per record**.[17]

57. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and theft of their PII/PHI;

b. The imminent and impending injury flowing from potential fraud

[17] "2018 Trustwave Global Security Report," TRUSTWAVE https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (last accessed December 12, 2022).

and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

58. Finally, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiffs and Class Members entered into agreements with and provided payment to Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI. Plaintiff and Class Members would not have entered into such agreements and would not have paid Defendant the amount that they paid had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that that do which they actually received.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiff intends to seek certification of the following Class, initially defined as follows:

> All persons residing in the United States of America who received a data breach notice informing them that their PII/PHI

had been breached by unauthorized third parties as a result of UGA's data breach.

60. Excluded from each of the above Classes is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

61. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that the joinder of all members is impractical. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

62. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
b. Whether Defendant violated common and statutory by failing to implement reasonable security procedures and practices;
c. Which security procedures and which data-breach notification

procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Defendant knew or should have known of the security breach prior to the disclosure;

e. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

g. Whether Defendant knew or should have known of the security breach prior to its disclosure;

h. Whether Defendant had a duty to promptly notify Plaintiff and Class Members that their PII was, or potentially could be, compromised;

i. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

j. The nature of the relief, including equitable relief, to which Plaintiff and the Class Members are entitled; and

k. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

63. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI/PII, like that of every other Class Member, was misused and/or disclosed by Defendant.

64. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intends to

prosecute this action vigorously. Plaintiff's claims are typical of the claims of other members of the Classes and Plaintiff has the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiff and his counsel.

65. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

66. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

67. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

68. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 67, inclusive, of this Complaint as if set forth fully herein.

69. Defendant requires any individual that uses its services to provide their PII and PHI to Defendant. Defendant collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

70. Defendant owed Plaintiffs and the Class Members a duty of care in the handling of its patient's PII/PHI. This duty included, but was not limited to, keeping that PII/PHI secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiffs and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

71. Defendant failed to implement "technology security plans and security software as party of an information security policy" as set forth under Georgia Code §10-1-910(4).

72. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII/PHI. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data

security obligations. [18]

73. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[19] NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.
>
> *Step 3: Create a Current Profile*. The organization develops a

[18] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last accessed January 10, 2023).

[19] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last accessed January 10, 2023).

Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to

determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

74. In addition to their obligations under state and federal regulations and industry standards, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and the Class Members.

75. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their internal data systems to ensure that the PII/PHI in Defendant's possession was adequately secured and protected.

76. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its custodianship, including adequately training its employees and others who accessed PII/PHI within its computer systems on how to adequately protect PII/PHI.

77. Defendant owed a duty to Plaintiff and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

78. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

79. Defendant owed a duty to Plaintiff and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiff and Class Members' decisions to entrust their PHI/PII to Defendants.

80. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occur.

81. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiff and the Class Members. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

82. Defendants breached its duties of care to safeguard and protect the

PII/PHI which Plaintiff and the Class Members entrusted to it. Upon information and belief, Defendant adopted inadequate safeguards to protect the PII/PHI and failed to adopt industry-wide standards set forth above in its supposed protection of the PII/PHI. Defendant failed to design, maintain, and test its computer system to ensure that the PII/PHI was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

83. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

84. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

85. As a direct and proximate result of Defendant's failure to adequately

protect and safeguard the PII, Plaintiff and the Class Members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

86. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Breach of Implied Contract

87. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 86, inclusive, of this Complaint as if set forth fully herein.

88. Plaintiff and Class Members entered into agreements for medical treatment with Defendant. In making those agreements, Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI to Defendant as requirement of receiving service. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Defendant would implement reasonable and adequate data security to safeguard and protect the PII and PHI entrusted to them by Plaintiff and Class Members from unauthorized disclosure.

89. Thus, when Plaintiff and Class Members provided their PII and PHI to Defendant in exchange for medical services, they entered into implied contracts with Defendant under which Defendant agreed to and was obligated to reasonably protect their PII and PHI. Plaintiff and Class Members provided payment to Defendant, as well as their PII and PHI, under the reasonable but mistaken belief that any money they paid to Defendant in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI.

90. This implied contract is acknowledged and memorialized in Defendant's customer-facing documents, including, *inter alia*, Defendant's online public-facing Privacy Policy, wherein it promises that "[w]e will obtain your express written authorization before using or disclosing your information for any other purpose not described in this notice."

91. Defendant did not provide reasonable and adequate data security for Plaintiff's and Class Member's PII and PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under implied contract.

92. That Defendant would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiff and Class Members. Reasonable consumers value the privacy of their PII and PHI, and do not enter into agreements for medical services with healthcare providers which are known not to protect customer data. Accordingly, Plaintiff and Class Members would not have entered into agreements with Defendant and would not have provided them with their sensitive PII and PHI, had they known that Defendant would not implement such reasonable and adequate data security.

93. As a result of Defendant's breach, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

94. Plaintiff and Class Members fully performed their obligations under the implied contract by providing their PII/PHI and making payments to Defendant.

95. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

Quasi-Contract/Unjust Enrichment

96. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 95, inclusive, of this Complaint as if set forth fully herein.

97. Plaintiff and Class Members provided their PII and PHI and conferred a monetary benefit upon Defendant in exchange for healthcare services. Plaintiffs and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII and PHI. Defendant was enriched when it sold its healthcare services at a higher price than it

otherwise would have based on those reasonable but mistaken beliefs.

98. Defendant's enrichment came at the expense of Plaintiff and Class Members, who would not have paid for Defendant's services, or would have only been willing to paid substantially less for them, had they been aware that Defendant had not implement reasonable, adequate and statutorily mandated safeguards to protect their PII and PHI.

99. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members suffered have suffered damages in the form of their lost benefit of the bargains. Plaintiff and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI. Plaintiff and Class Members would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

100. Defendant should not be permitted to retain Plaintiff's and Class Members' lost benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Defendant should not be allowed to benefit at the expense of consumers who trust Defendant to protect the PII and PHI that they are required to provide to Defendant in order to receive Defendant's services.

101. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an

amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

FOURTH CAUSE OF ACTION

Breach of Fiduciary Duty

102. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 101, inclusive, of this Complaint as if set forth fully herein.

103. Plaintiff and Class Members provided their PII and PHI to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of that information. Plaintiffs and Class Members would not have provided Defendant with their PII and PHI had they known that Defendant would not take reasonable and adequate steps to protect it.

104. Defendant's acceptance and storage of Plaintiff's and Class Members' PII and PHI created a fiduciary relationship between Defendant and Plaintiffs and Class Members. As a fiduciary of Plaintiffs and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiff's and Class Members' PII and PHI.

105. Defendant breached its fiduciary duties to Plaintiff and Class Members by, *inter alia,* failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security training for its employees, and otherwise failing to reasonably and adequately safeguard the PII and PHI of Plaintiffs and Class Members.

106. As a direct and proximate result of Defendant's breaches of its fiduciary

duties, Plaintiff and Class Members have suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

107. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

1. For an Order certifying the Classes as defined herein and appointing Plaintiff and his Counsel to represent the Classes;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate

methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.

4. For an award of damages, including actual and compensatory damages, in an amount to be determined at trial;

5. For an award of punitive and treble damages, in an amount to be determined at trial;

6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

7. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: January 10, 2023

Counsel for Plaintiffs,

/s/ *Sharon J. Zinns*
Sharon J. Zinns
sharon@zinnslaw.com
Georgia Bar No. 552920

ZINNS LAW, LLC
1800 Peachtree St. NW, Suite 370
Atlanta, GA 30309
Tel: (404) 882-9002

/s/ *Thiago M. Coelho*
Thiago M. Coelho*
thiago@wilshirelawfirm.com
California Bar No. 324715
**Pro Hac Vice to be filed*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., FL 12
Los Angeles, CA 90010
Tel: (213) 381-9988
Fax: (213) 381-9989

FONT CERTIFICATION

Pursuant to Local Rule 7.1(D), I hereby certify that the foregoing document was prepared using Times New Roman 14 point type as specified in Local Rule 5.1(C).

Dated: January 10, 2023

Respectfully Submitted,

/s/ *Sharon J. Zinns*

Sharon J. Zinns
sharon@zinnslaw.com
Georgia Bar No. 552920

ZINNS LAW, LLC
1800 Peachtree St. NW, Suite 370
Atlanta, GA 30309
Tel: (404) 882-9002

/s/ *Thiago M. Coelho*

Thiago M. Coelho*
thiago@wilshirelawfirm.com
California Bar No. 324715
**Pro Hac Vice to be filed*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., FL 12
Los Angeles, CA 90010
Tel: (213) 381-9988
Fax: (213) 381-9989